FAT ERASER

มหาภัย จาก ไวรัสพันธุ์ใหม่

ลิขิต ชัยกิจ

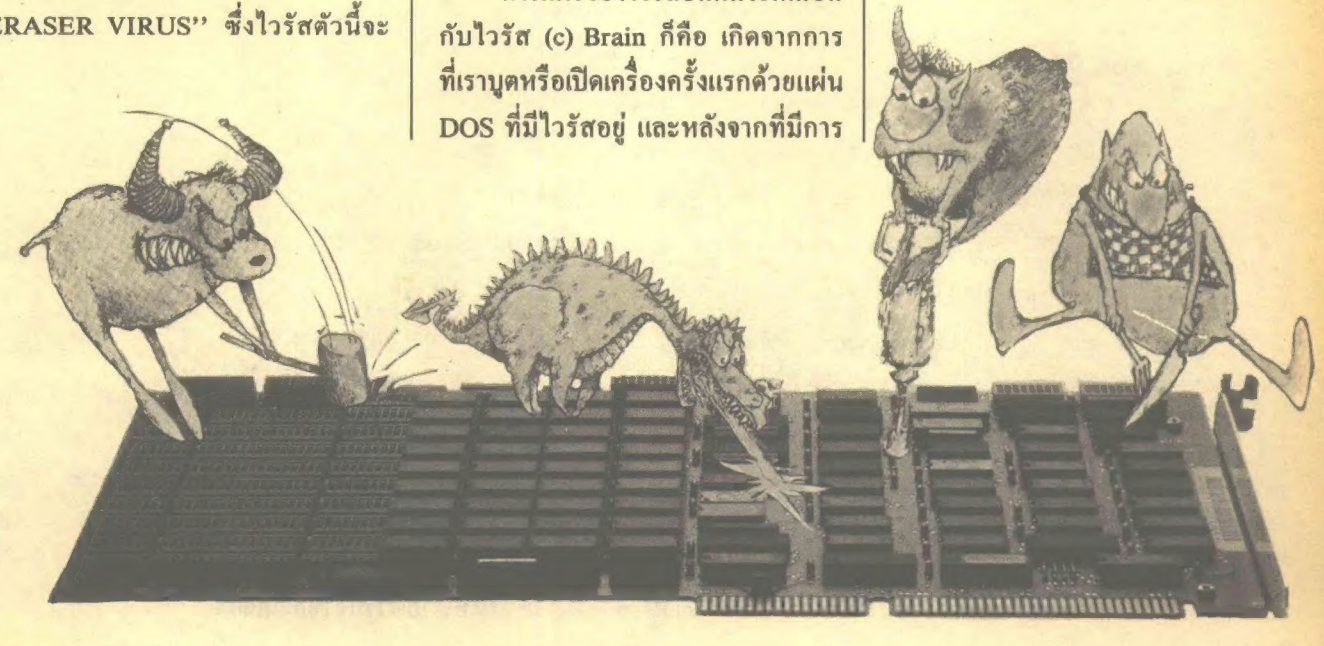
จากการที่ได้มีการกล่าวขวัญเรื่องไวรัส (c) Brain กันมากเมื่อไม่นานมานี้ มาในครั้งนี้ก็จะเสนอให้ผู้อ่านรู้จักกับไวรัสอีกครั้งหนึ่ง ซึ่งถ้าจะเปรียบกับ (c) Brain แล้วดูไปจะค่อนข้างร้ายแรงกว่า และวิธีการแพร่ของไวรัส ชนิดนี้ก็เป็นอีกแบบหนึ่งซึ่งไม่เหมือนกับ (c) Brain

จากการที่ได้ศึกษามานั้น ไวรัสชนิดนี้ไม่มีชื่อที่แท้จริง ทีมงานของเราจึงได้ตั้งชื่อไวรัสชนิดนี้ว่า "FAT ERASER VIRUS" ซึ่งไวรัสตัวนี้จะอยู่ในบูตเซกเตอร์เช่นเดียวกับ (c) Brain แต่ไวรัสชนิดนี้สังเกตยากมาก เพราะการทำงานของดิสค์ไดรฟ์จะไม่ช้าลง และจะไม่มีการเปลี่ยน Volume Label ของดิสค์ให้เห็นเหมือนกับไวรัส (c) Brain ในขณะเดียวกันไวรัสชนิดนี้จะไม่ปรากฏข้อความใด ๆ ให้เป็นที่สงสัยในเซกเตอร์แรกของดิสค์

การแพร่ของเชื้อ FAT ERASER VIRUS

การแพร่ของไวรัสชนิดนี้จะเหมือนกับไวรัส (c) Brain ก็คือ เกิดจากการที่เราบูตหรือเปิดเครื่องครั้งแรกด้วยแผ่น DOS ที่มีไวรัสอยู่ และหลังจากที่มีการเปิดเครื่องดังกล่าวแล้ว ไวรัสก็จะทำการเข้าไปฝังตัวอยู่ในหน่วยความจำของเครื่อง ซึ่งจะกินหน่วยความจำเท่าไหร่ก็ขึ้นอยู่กับชนิดของไวรัสนั้น ๆ

แต่การแพร่ขยายของ FAT ERASER VIRUS นี้จะทำเพียงเมื่อ ปุ่ม CTRL-ALT-DEL ถูกกดเพื่อจะ RESET เครื่องแล้วใส่แผ่นใหม่ที่ไม่มีไวรัสเข้าไป แผ่นใหม่ดังกล่าวก็จะติดไวรัสทันทีถ้าไม่มี Write Protect และข้อพิเศษของไวรัสชนิดนี้คือ ไวรัส



จะไม่หายไปโดยการ กด CTRL-ALT-DEL แต่จะหายก็ต่อเมื่อเปิดเครื่องหรือกดปุ่มรีเซตด้วยแผ่น DOS ที่ไม่มีไวรัสอยู่

ผลการติดเชื้อ FAT ERASER VIRUS

1) ไวรัส จะกินเนื้อที่ในหน่วยความจำของเครื่องไป 1 กิโลไบต์

2) ทำลาย FAT (File Allocation Table) ในแผ่นดิสค์โดยทำให้โค้ดต่าง ๆ ใน FAT เปลี่ยนค่าไปจากเดิม (FAT เป็นตัวบอกตำแหน่งของข้อมูลและโปรแกรมต่าง ๆ บนแผ่นดิสค์นั้น) ซึ่งถ้า FAT ถูกทำลายแล้ว เราก็จะไม่สามารถอ่านข้อมูลในดิสค์แผ่นนั้นได้ครบถ้วนอีกต่อไป และที่ร้ายที่สุดก็คือเมื่อเสียไปแล้ว โอกาสที่จะทำให้กลับคืนมาเป็นปกติแทบจะไม่มีเลย

ดังนั้นจึงจำเป็นอย่างยิ่งที่ควรจะรีบกำจัดไวรัสตัวนี้และตัวอื่นให้หมดไปก่อนที่จะเกิดความสูญเสียแก่ข้อมูลหรือโปรแกรมของท่านเป็นมูลค่าที่ประเมินไม่ได้ เพราะเหตุนี้ทีมงานของเราจึงได้ร่วมกันทำโปรแกรมชุดหนึ่งขึ้นมา ให้มีความสามารถที่จะกำจัดไวรัสชนิดนี้ รวมถึงไวรัส (c) Brain ตัวเก่าอีกด้วย พร้อมกับโปรแกรมชนิดนี้ยังสามารถทำการป้องกันไม่ให้ไวรัสชนิดนี้ และ (c) Brain ติดเข้าไปในแผ่นของท่าน ซึ่งเปรียบเสมือนเป็นการ ฉีดวัคซีนป้องกันไวรัสก็ว่าได้ ซึ่งโปรแกรมกำจัดไวรัสทีมงานเราได้ตั้งชื่อว่า VIRUS LAB

การตรวจสอบและการกำจัดไวรัส

ท่านสามารถใช้โปรแกรม PC-TOOLS เวอร์ชั่นใดก็ได้ ในการค้นหาและตรวจดูไวรัสบนแผ่นดิสค์และถ้าจะใช้ในการกำจัดไวรัสก็ควรจะเพิ่มความระมัดระวัง เพราะถ้าทำไม่ดีอาจจะทำให้ข้อมูลทั้งหมดนั้นเสียไปหมดจนไม่สามารถที่จะแก้ไขได้อีกเลย อย่างเช่นถ้าท่านต้องการตรวจดูว่าในเครื่องของท่านตอนนี้มีไวรัสฝังตัวอยู่ในหน่วยความจำหรือไม่ ท่านสามารถใช้ฟังก์ชัน System Info ตรวจดูได้ ซึ่งจะปรากฏบนหน้าจอเป็นดังรูปที่ 1

นอกจากโปรแกรม PCTOOLS แล้ว ท่านอาจจะใช้โปรแกรมอื่น ๆ ก็ได้

```
PC Tools Deluxe R4.11    <- สามารถใช้ เวอร์ชั่น อื่นก็ได้
-------------------- System Information Service --------------------
                                Computer - IBM/PC
            The BIOS programs are dated - 08/16/82
                        Operating system - DOS 3.20
          Number of logical disk drives - 5
             Logical drive letter range - A thru E
                           Serial Ports - 1
                         Parallel Ports - 2
                                CPU Type - 8088
          Relative speed (orig PC=100%) - 210%
              Math co-processor present - No
User programs are loaded at HEX paragraph - 0AE3
 Memory used by DOS and resident programs - 44592 bytes
      Memory available for user programs - 610768 bytes
           Total memory reported by DOS - 640 K    <- หน่วยความจำเต็ม
PC Tools has found the total memory to be - 639 K    <- แสดงให้เห็นว่าหน่วยความจำ
Monochrome Display Adapter present                    ถูกกินไป 1 K

Press any key to return
```

รูปที่ 1 บนจอภาพแสดงให้เห็นว่า มี FAT Eraser VIRUS ฝังตัวอยู่ในหน่วยความจำของเครื่อง

อย่างเช่นของ Peter Norton เป็นต้น

แต่ถ้าท่านใช้ Virus Lab ดังกล่าวนี้ ท่านสามารถตัดความยุ่งยากทั้งหลายไปได้หมดและโปรแกรมชุดนี้ยังง่ายต่อการใช้ เพียงแค่ท่านอ่านข้อความที่ให้ไว้ ท่านก็สามารถทำเองได้เลย

รู้จักกับโปรแกรม VIRUS LAB

โปรแกรมนี้ได้ถูกพัฒนาขึ้นโดยทีมงานของ Sphinx Software Lab มีคุณลิขิต ชัยกิจ และนักเรียนโรงเรียนแอ็ดเวนตีสเป็นผู้จัดทำ โดยโปรแกรมนี้ถูกเขียนเป็นภาษาแอสเซมบลี

คุณสมบัติพิเศษของ VIRUS LAB

1) สามารถบอกได้ว่าในแผ่นดิสเกตต์ของท่านมีไวรัสชนิดไหนอยู่

2) สามารถกำจัดไวรัส (c) Brain และ FAT ERASER ในเวลาที่รวดเร็ว

3) สามารถทำให้แผ่นดิสเกตต์ของท่านไม่ถูกไวรัสแพร่ใส่อีก โดยใช้ VACCINE ของโปรแกรมนี้ ถึงแม้แผ่นของท่านจะไม่ติด Write Protect ก็ตาม

4) สามารถตรวจสอบว่า ในหน่วยความจำของเครื่องที่ท่านใช้อยู่มีไวรัสฝังตัวอยู่หรือไม่

หลักการทำงานของโปรแกรม VIRUS LAB Version 1.10

ในการกำจัดไวรัสที่มีอยู่ในแผ่นดิสก์นั้น โปรแกรมจะทำการค้นหาว่า

ในแผ่นนั้นมีไวรัสอยู่หรือไม่ ถ้ามีก็จะค้นหาอีกว่าเป็นไวรัสชนิดไหน เพราะวิธีการกำจัดไวรัสแต่ละชนิดนั้นไม่เหมือนกัน ซึ่งโปรแกรมนี้สามารถกำจัดไวรัสได้ 3 ชนิด คือ

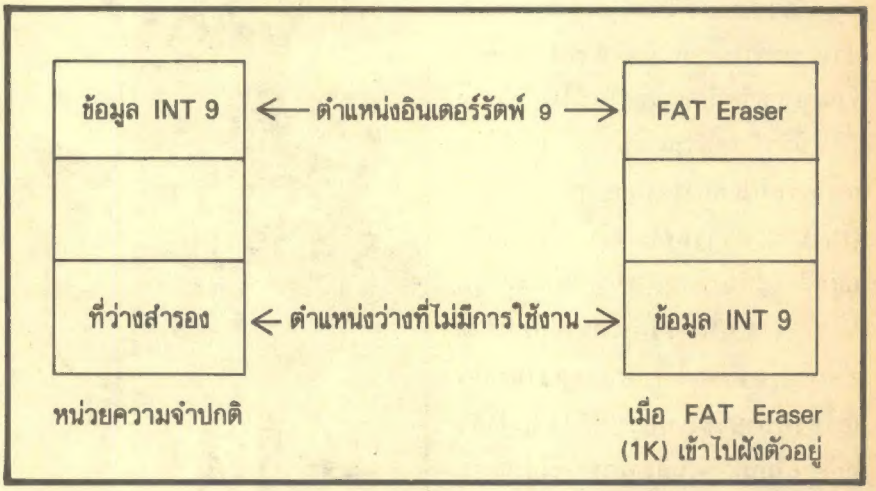
1. ไวรัสชนิด A คือ (c) Brain
2. ไวรัสชนิด B คือ FAT Eraser Virus (1K)
3. ไวรัสชนิด B+ คือ T2

ไวรัสในข้อ 3 นั้น เป็นไวรัสอีกชนิดที่เพิ่งพบเห็น ซึ่งมีการทำงานที่คล้ายคลึงกับไวรัสชนิด B (FAT Eraser Virus) มาก จากที่ได้มีการศึกษามานั้น ไวรัสชนิด B+ อาจจะเป็นไวรัสที่มีคนแก้ไขเพิ่มจากไวรัส ชนิด B จนทำให้เป็นไวรัสชนิดใหม่ขึ้น แต่ที่ร้ายกว่าคือ ไวรัสชนิด B+ (T2) จะฟอร์แมต FAT ทั้งหมด แทนที่จะเปลี่ยนไบต์บางตัวใน FAT ส่วนการแพร่ก็เหมือนกัน คือจะแพร่เมื่อมีการกด (Ctrl)+(Alt)+(Del) และมีการฝังตัวในที่เดียวกัน

การฝังตัวของไวรัส ทั้ง 2 ชนิดนี้ (FAT Eraser Virus and T2)

ไวรัสดังกล่าวจะเข้าไปฝังตัวในแผ่นนั้น ไวรัสชนิดนี้จะเข้าไปอยู่ในตำแหน่งเซกเตอร์ 0 หรือที่เรียกว่า "Boot sector" นั่นเอง และไวรัสก็จะย้ายบูตเซกเตอร์จริงไปอยู่ในตำแหน่งเซกเตอร์ 709 ทุกครั้งไม่ว่าในตำแหน่งดังกล่าวจะมีข้อมูลอยู่หรือไม่ ซึ่งถ้ามีข้อมูลอยู่ในตำแหน่งนั้นข้อมูลก็จะถูกทับโดยข้อมูลในบูตเซกเตอร์ที่ถูกย้ายมาโดยไวรัสนั่นเอง

ดังนั้นการกำจัดไวรัสชนิดนี้ออกไปจากแผ่น สามารถกระทำได้โดยการย้ายข้อมูลในเซกเตอร์ที่ 709 ลงมาทับในเซกเตอร์ 0 เหมือนเดิม เท่านี้ไวรัสทั้งสองชนิดก็จะถูกกำจัดไปโดยปริยาย



รูปที่ 2 แสดงการเข้าไปฝังตัวในหน่วยความจำของไวรัส FAT Eraser Virus (1K)

ส่วนการป้องกัน FAT Eraser virus นี้เป็นเรื่องที่ค่อนข้างยาก เพราะการตรวจสอบของไวรัสชนิดนี้ว่า ในดิสก์แผ่นนั้นเป็นแผ่นชนิดเดียวกับแผ่นของไวรัสชนิดนั้นหรือไม่คือ การตรวจสอบของไวรัส (c) Brain นั้นจะดูที่ไบต์ 4 และ 5 เท่านั้น แต่ใน FAT Eraser virus นั้น มันจะดูเซกเตอร์ 0 ทั้งเซกเตอร์ โดยปกติของการเปิดเครื่องหรือบูตเครื่องทุกครั้งเครื่องจะนำเอาข้อมูลในเซกเตอร์ 0 หรือ System ในแผ่นนั้น ๆ ลงไปฝังตัวในหน่วยความจำ และยิ่งถ้าในแผ่นที่บูตเครื่องนั้นมีไวรัสอยู่ในแผ่นด้วยแล้วละก็ ไวรัสก็จะเข้าไปฝังตัวในหน่วยความจำ เช่นเดียวกันคือในหน่วยความจำก็จะมีข้อมูล system และ ตัวไวรัสอยู่ด้วยกัน

การตรวจสอบแผ่นของไวรัส FAT Eraser virus นี้จะทำการตรวจสอบดูว่าข้อมูล system ที่ถูกโหลดลงมาฝังตัวอยู่ในหน่วยความจำกับข้อมูลที่อยู่ในแผ่นในเซกเตอร์ 0 นั้นเหมือนกันหรือไม่ ซึ่งเป็นการยากมากที่เราจะทำการป้องกันไวรัสชนิดนี้ เพราะตามปกติในแผ่นดิสก์แต่ละแผ่นก็จะมีข้อมูลหรือ system ในเซกเตอร์ 0 ที่แตกต่างกันไป

ดังนั้นการป้องกันวิธีที่ง่าย ๆ ก็สามารถทำได้โดย ปิด Write protect ที่แผ่น หรือเปิดเครื่องใหม่โดยใช้แผ่นที่ไม่มีไวรัสอยู่ในแผ่นนั้น (อย่าบูตเครื่องใหม่โดยการ กด (Ctrl)+(Alt)+(Del) การตรวจสอบว่าแผ่นนั้นมีไวรัสอยู่หรือไม่นั้น ท่านสามารถใช้โปรแกรม VIRUS LAB ในการตรวจสอบดูได้ ส่วนการตรวจดูว่าในหน่วยความจำในเครื่องที่ท่านใช้งานอยู่นั้นมีไวรัสฝังตัวอยู่หรือไม่นั้น ท่านก็สามารถใช้โปรแกรม VIRUS LAB ตรวจได้ เพราะโปรแกรม VIRUS LAB เวอร์ชั่น 1.10 จะไม่ทำงานถ้าในหน่วยความจำในเครื่องที่ท่านกำลังใช้งานอยู่นั้นมีไวรัสฝังตัวอยู่ โดยโปรแกรมจะทำการแจ้งให้ท่านทราบทันทีว่า ในเครื่องของท่านตอนนี้มีไวรัสฝังตัวอยู่

นอกจากนี้แล้ว ทีมงานของเรายังมีโปรแกรมย่อยอีก 2 ตัว คือ "AV-Format" กับ "AV-Inject"

AV-FORMAT

โปรแกรมนี้มีความสามารถเช่นเดียวกับโปรแกรม FORMAT ของ DOS Version 3.3 คือ ฟอร์แมตแผ่นและมีพารามิเตอร์ (/v/s/1...) เหมือนกันทุกประการ แตกต่างกันเพียง AV-FORMAT จะป้องกันไวรัส หลังจากที่ฟอร์แมตแผ่นเรียบร้อยแล้ว และดิสก์แผ่นนั้นจะไม่ติดไวรัสอีกเลย

AV-INJECT

โปรแกรมนี้คล้ายคลึงกับ AV-FORMAT แต่ใช้กับดิสก์ที่มีข้อมูลอยู่แล้ว (ไม่ต้องการฟอร์แมต) และจะป้องกันไม่ให้ติดไวรัสอีกเช่นกัน

เทคนิคการป้องกันไวรัสของการ Inject

โดยการเปลี่ยนข้อมูลในบูตเซกเตอร์ ณ ตำแหน่งไบต์ที่ 4 กับ 5 ซึ่งเปลี่ยนแล้วจะไม่กระทบกระเทือน การบูตตามปกติแต่อย่างใด และเมื่อไบต์ที่ 4 กับ 5 ถูกเปลี่ยนให้เหมือนกับไวรัสแล้ว เมื่อไวรัสกำลังจะเขียนตัวของมันเองลงในดิสก์ มันจะอ่านตำแหน่งที่ได้กล่าวไว้ข้างต้น เพื่อตรวจดูว่ามีไวรัสชนิดเดียวกับตัวของมันอยู่หรือไม่ ถ้ามีมันจะไม่เขียนทับลงไปอีก สรุปคือไบต์ที่ 4 และ 5 ของบูตเซกเตอร์จะเป็นตัวบอกว่าดิสก์นี้มีไวรัสหรือไม่ ซึ่งค่าที่อ่านได้คือ 1234 (เลขฐาน 16)

หมายเหตุ : ไวรัสที่ตรวจดูเพียงไบต์ที่ 4 กับ 5 เพื่อหาตัวมันเองนั้นคือ ไวรัสชนิด A: (c) Brain และไวรัสชนิด C: Den Zuk เท่านั้น ส่วนไวรัสชนิดอื่นที่มีวิธีการตรวจหาที่แตกต่างจาก 2 ตัวนี้ วิธีการข้างต้นนี้จะไม่สามารถป้องกันได้

โปรแกรมชุดนี้ทีมงานของเรายินดีอย่างยิ่งที่จะมอบเป็นสาธารณประโยชน์ ถ้าท่านสนใจสามารถดูรายละเอียดได้จากคอลัมน์ซอฟต์เมล์ประจำฉบับ หรือติดต่อโดยตรงถึง ทีมงานของเราได้ที่

ลิขิต ขัยกิจ
127/1 ซอยเจริญใจ เอกมัย พระโขนง
กรุงเทพฯ 10110
เบอร์โทรศัพท์ : 3916340
อรรถพันธ์ อารยะสันติภาพ
ซอย 2 หมู่บ้านสวนสน สุขาภิบาล 2
บางกะปิ กรุงเทพฯ 10240
เบอร์โทรศัพท์ : 3745294